View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Explore Bristol Research

Hugues Salas, E., Ntavou, F., Gkounis, D., Kanellos, G., Nejabati, R., & Simeonidou, D. (2019). Monitoring and Physical-Layer Attack Mitigation in SDN-Controlled Quantum Key Distribution Networks. *IEEE/OSA Journal of Optical Communications and Networking*, *11*(2), A209-A218. [2]. https://doi.org/10.1364/JOCN.11.00A209

Peer reviewed version

Link to published version (if available):
10.1364/JOCN.11.00A209

Link to publication record in Explore Bristol Research
PDF-document

This is the author accepted manuscript (AAM). The final published version (version of record) is available online via OSA at https://www.osapublishing.org/jocn/abstract.cfm?uri=jocn-11-2-A209. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research
General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available:
http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/

Monitoring and Physical Layer Attack Mitigation in SDN-Controlled Quantum Key Distribution (QKD) Networks

Emilio Hugues-Salas, Foteini Ntavou, Dimitris Gkounis, George T. Kanellos, Reza Nejabati and Dimitra Simeonidou

Abstract*— Quantum Key Distribution (QKD) has been identified as a secure method for providing symmetric keys between two parties based on the fundamental laws of quantum physics, making impossible for a third party to copy the quantum states exchanged without being detected by the sender (Alice) and receiver (BoB) and without altering the original states. However, when QKD is applied in a deployed optical network, physical layer intrusions may occur in the optical links by injecting harmful signals directly into the optical fibre. This can have a detrimental effect on the key distribution and eventually lead to its disruption. On the other hand, network architectures with software defined networking (SDN) benefit from a homogeneous and unified control plane that can seamlessly control a QKD enabled optical network end-to-end. There is no need for a separate QKD control, a separate control for each segment of an optical network and an orchestrator to coordinate between these parts. Furthermore, SDN allows customised and application tailored control and algorithm provisioning, such as QKD aware optical path computation, to be deployed in the network, independent of the underlying infrastructure. Therefore, in this manuscript, we investigate the integration of the application, SDN and QKD infrastructure layers and confirm capability for flexible supervision and uninterrupted key service provisioning in the event of link level attacks. An experimental demonstrator is used, for the first time, to verify the architecture proposed, considering real-time monitoring of quantum parameters and fiber-optic link intruders to emulate real-world conditions. Furthermore, attacks on a standard single-mode fiber (via a 3dB coupler) and a multicore fiber (via an adjacent core) are undertaken to explore different connectivity between QKD units. Results show an additional attacker identification and switching time of less than 60ms for the link cases investigated, being negligible compared to the total (re)-initialization time of 14 minutes of the QKD units.

***Index Terms*—software defined networking, quantum key distribution, multicore fiber, link failure mitigation**

I. Introduction

Current optical networks integrate different domains (e.g. core, metro, access) over an optical fiber platform to fulfill the requirements of large capacity, low power consumption and longer reach [1]. This characteristic of large data rate permitted by the fiber optic is also required in modern data centers where the growth of IP traffic occurs at a rate of 25% every year and will continue until a total of 20.6 zettabytes is reached by 2021 [2]. However, these complex and high-bandwidth networks based on optical fiber connections are susceptible to security breaches since the data from the optical fiber can be tapped without being detected. To this end, security in optical networks relies on different encryption methods, with Advanced Standard Encryption (AES) being one of the most used [3]. This method encrypts data with a secure key of 128 or 256 bits size, to convert the data in a cyphertext.

A strong candidate for data encryption in installed optical networks is quantum key distribution (QKD) [4]. QKD is foreseen as an important technique for sharing cryptographic keys in present and future secure communication networks [5]. In optical networks, QKD relies on the generation and distribution of symmetric keys by transmitting single photons from a sender, Alice, to a receiver, Bob, over an optical channel. Any eavesdropping attempt by Eve can be detected because measuring a photon on which a key bit is encoded, will cause an irreversible change. Thus, QKD offers advanced security features as a result of the fundamental constraints prescribed by quantum mechanics.

However, QKD sensitivity to the optical losses and the noise level of the links increase the technology susceptibility against physical-layer attacks and becomes the main security threat in optical QKD networks [6,7]. An attack over an individual optical fiber link can be executed by acting on the quantum channel, increasing the noise above the threshold of security and disrupting the key generation, despite the availability of the QKD link. Denial of service (DoS) attacks have been identified as a QKD vulnerability in [8] since QKD easies the disruption of secure transmissions due to abortion of key generation whenever tampering is detected. Nevertheless, with the availability of several optical paths within a network with

QKD resources, the mitigation of attacks is envisaged as described in [7].

Various approaches integrating QKD in a network scale have been successfully demonstrated worldwide including field trials [9-12]. However, optical networks are continuously evolving to complex network architectures requiring advanced programmability. Software defined Networking (SDN) fulfills this programmability and network management needs since SDN decouples the control plane from the data plane, enabling an end-to-end flexible configuration of the data plane devices from a centralized control entity, called the SDN controller, as well as a more efficient orchestration and automation of the network services [13]. Based on this centralized controller, SDN has the capability to respond to continuous demand of network resources since the entire information of the network is contained in one network operating system [14]. These SDN feature allows for it to be used as a converged network control mechanism that can simultaneously and in a coordinated manner control different segments of an end-to-end optical network (core, access, metro) and its associated networking systems such QKD security. Furthermore, it allows deployment for customized network control algorithms independent of underlying infrastructure such as load balancing, network slicing or QKD-aware path computation.

These SDN functionalities are the key motivator for the integration of QKD in an SDN-enabled optical network, as shown in [15,16,17,18,19,20,21]. The current works have proved that the SDN integration is beneficial for the QKD networks for customized network configuration (e.g. path computation algorithm) for optimum QKD performance. In particular, in [22] it has been demonstrated that the combination of QKD and SDN can provide continuous real-time monitoring of quantum parameters, such as quantum bit error rate (QBER) and secret key rate (SKR), and flexible configuration of optical paths to ensure the uninterrupted distribution of quantum keys in a network prone to physical-layer attacks or with randomly appearing physical impairments.

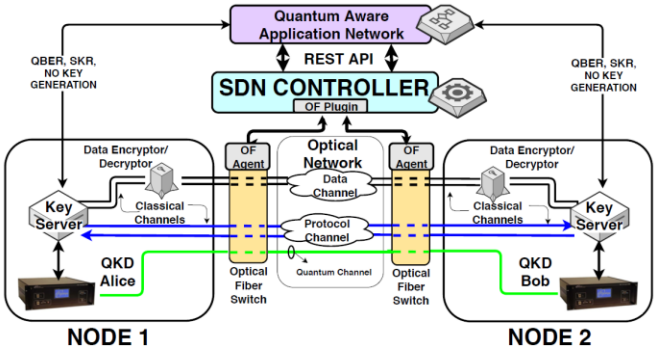

Fig. 1. Quantum key distribution supported by software defined networking with real-time monitoring

However, most of the QKD network demonstrations to date utilize a dedicated dark fiber, with single photons being transmitted over a separate optical fiber path. Classical optical modulated signals exhibit more than eight orders of magnitude of additional power in comparison to the quantum signal. This high power present on the classical channels generates noise that proliferates across wavelengths, prohibiting the transmission of encoded photons and the generation of keys across the same optical fiber [23,24]. This impacts the network infrastructure since additional optical fibers are required for transmission of the classical data, adding complexity and cost to existing networks. On the other hand, significant progress on multicore fiber (MCFs) technologies has allowed the consideration of space-division multiplexing (SDM) concepts as a viable solution in multi-dimensional networking [25]. To this end we propose and study MCFs as the SDM enabling solution that allows not only the classical and quantum channels coexistence in a natural manner without deploying surplus fiber links [26], but also the enhancement of the attack mitigation techniques using SDN as a platform to select an alternative secure path.

In this paper, the practical investigation of physical-layer intrusions over quantum channels is presented in combination with SDN for mitigating the attack and provision of continuous secure connectivity of QKD units. In addition, to the best of the authors' knowledge, attacks over quantum channels have not been investigated in SDM (MCF) and in this work, the experimental demonstration has been used to verify the impact and to probe the mitigation technique using SDN and real-time monitoring. This work details the concept of a SDN-based network control application suitable for mitigating a channel attack in a QKD network and extends the results of [22] with further investigations of the impact of the optical fiber length in SSMF, the effect of wavelength-tuning the attacker and the result of crosstalk in MCFs and inter-core MCF switching after adjacent-core attack. Characterization of the MCF is shown as well as fundamental descriptions of the encryption operation with respect to key material. This work is organized as follows: in section II of this paper, we review the physical layer security in traditional optical networks and MCF-based networks, in section III we present the QKD system architecture, in section IV, the optical network components for QKD are described followed by section V with the QKD scenarios supported by SDN. Section VI includes the implemented physical layer attackers and section VII describes the experimental results. Finally, section VIII concludes the manuscript.

II. Review of Physical Layer Security over Optical Fibers

Service disruption and eavesdropping are the main effects of physical layer attacks. In [27,28] three types of attacks are highlighted: *i)* signal insertion attacks, *ii)* signal splitting attacks and, *iii)* physical infrastructure attacks. In the signal insertion attacks, destructive signals are added into the fiber network, causing service degradation. These attacks can potentially cause DoS, isolating nodes due to the low quality of transmissions. High-powered jamming attacks, with power levels of 5-10dBs above the typical power can be inserted into optical channels used within the network (in-band jamming) or in channels beyond the network use (out-of-band jamming). Physical impairments such as nonlinearities and crosstalk can occur due to these attacks. Moreover, these nonlinearities can be a consequence of flexi-grid networks with combined line rates and modulation formats. From the installation and

implementation point of view, network sites are vulnerable to malicious operation where the power level of the lasers can be modified, and harmful signals can be inserted in patch panels. Besides, monitoring ports in amplifiers, wavelength selective switches (WSSs) and optical switches can be an attractive attacking insertion point since access to signals is undertaken by splitters.

Signal splitting attacks arise whenever the attacker split or remove part of the signal carried in the network. This splitting provokes signal eavesdropping or degradation and suitable detection of this kind of attacks is difficult. On the optical fiber side, by manipulating the fiber cladding and bending the fiber, light can be radiated to a monitoring device for eavesdropping.

The third type corresponds to physical infrastructure attacks which are all the attacks that damage or tamper the optical network infrastructure, i.e. cutting a fiber, unplugging connections or destroying optical components.

With regards to SDM, physical layer attacks have recently been studied in [29,30]. Essentially, a transmitting signal over a single core of an MCF will suffer from the crosstalk induced by the attack in an adjacent core created by an incoming optical signal. The amount of inter-core crosstalk will depend on the position and direction of the attacked core with respect to the core selected for signal transmission [31]. In [29], results show that individual MCF connections are highly vulnerable to the high-power jamming attacks, especially the ones with more complex modulation formats or longer reaches. In addition, the effect of the jamming attacks is more noticeable at the network level with significant number of data connections being disrupted. In [30], attack-aware routing, spectrum and core assignment algorithms are proposed, prioritizing to avoid physical-layer security threats and to try to reduce the crosstalk-induced impairments.

alternative_quantum_channel_paths	[table]
id	INTEGER
sitename	TEXT
connected_sitename	TEXT
distance	INTEGER
optical_switch_left_id	TEXT
optical_switch_left_port	TEXT
optical_switch_right_id	TEXT
optical_switch_right_port	TEXT
connected	INTEGER

Fig. 2. Database schema for storing the alternative paths of the quantum channel

III. QKD SYSTEM ARCHITECTURE

Fig. 1 shows the key components of the proposed architecture of a real-time monitored QKD system over a software-defined optical network. This approach follows the traditional SDN architecture with an infrastructure layer, a control layer and an application layer. The infrastructure layer comprises of QKD units, Layer 2 encryptors/ decryptors and optical switches. The SDN controller lies in the control layer and manipulates the data layer through the southbound interface, (i.e. OpenFlow). All the software applications that leverage the advantages of the SDN controller and are responsible for the decision-making remain in the application layer and communicate with the SDN controller through the northbound interface, in our case the Representational State Transfer-Application programming interface (REST API). Information about all the different components of the proposed architecture, are summarized in Table I.

TABLE I.
System Specifications

MCF Parameters	**Value**
Fibre Type	Step Index Core Multicore Fibre
Mode Field Diameter (MFD)	10.3μm @1550nm
Propagation Loss	0.2dB/km @1550nm
Inter-core crosstalk	-48dB/1000m @1550nm
Core Pitch	44.7μm (average)
QKD Device Parameters	**Value**
Model	Clavis2, IDQuantique
Laser Wavelength	1552nm
QKD Protocol	BB84
Distance (Maximum)	50Km@10dB of loss
Secret Key Rate	> 500 bps over 25 km
Encryptors	**Value**
Model	Centauris, IDQuantique
Encryption algorithm	AES 256 GCM
Key refreshment period	1min
Link 1 Characteristics	**Value**
Fibre Type	SSMF
Link Length	500m/2km
Link Power Loss	4.2dB
Link 2/3 Characteristics	**Value**
Fibre Type	7core - MCF
Link Length	1km
Link Power Loss	4dB
Link 4 Characteristics	**Value**
Fibre Type	SSMF
Link length	515m
Link Power Loss	6.14dB
Number of hops	2
SDN controller	**Value**
SDN controller version	OpenDaylight Lithium
Southbound Interface	OpenFlow 1.0
Northbound Interface	REST API

IV. QKD OPTICAL NETWORK COMPONENTS

The components for the distribution of quantum-secured keys are illustrated in Fig. 1. Node 1 includes an Alice QKD unit (Clavis2, IDQuantique [32]), and a key server (running Linux). In an analogous way, Node 2 contains a Bob QKD unit and a key server. Typically, in an optical network infrastructure, two QKD nodes will be interconnected by different optical links where optical components as well as optical fibers will be selected to optimize the power budget and to avoid any possibility of noise interference due to optical amplifiers. In this network architecture, an optical fiber (or core of the MCF) is dedicated to the quantum channel that will be used for the transmission of the encoded photons. The classical channels (i.e. channels used for the QKD protocol and data transmission), are also assigned to optical fiber links where a pair of fibers is required for bidirectional transmission and reception.

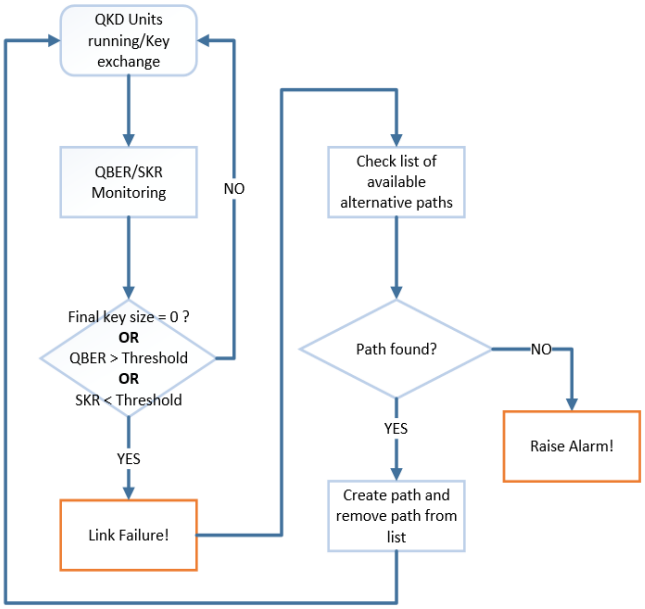

Fig.3. Workflow of the QPA decision making for the link failure mitigation

A. *Data transmission encryption*

Fig. 1 depicts the data transmission channels, which are also interfacing an optical fiber network. Layer 2 encryptors/decryptors (Centauris CN8000, IDQuantique [33]) are used in both nodes of Fig. 1 and are connected optically to the respective key servers. The traffic sent by the servers to the encryptors is ciphered with a 256-bit key received from the QKD units, using AES-256 GCM encryption. The encrypted data is then transferred to the end-node and decrypted using the same symmetric key. The key used in the encryption is refreshed every 1 minute, but this can be adapted according to the requirements of the system. The more frequent the key is refreshed, the more secure the encryption becomes. However, the frequent key refreshment could decrease the network throughput and lead to an exhaustion of the key material in the buffers [34]. In case of a quantum-channel attack, the encryptors will continue to use QKD keys that were previously generated and are saved in the key buffer of the key server. This buffer can be filled with a maximum of 1Mbits of key material before the buffer needs to be refreshed with new key material.

B. *Quantum parameters monitoring and SDN implementation*

The key enabling technology used in this proposed network architecture is the software-defined optical network [13]. The control of the network is achieved through an SDN controller with a network-wide view. The SDN controller uses open APIs to configure the different network devices, thus enabling a dynamic QKD network configuration. To further enhance the capabilities of SDN, a Quantum Parameters Monitor (QPM) application is also introduced. The application enables the real-time monitoring of the important parameters for the QKD system's performance, such as the SKR and the QBER. The QPM application analyzes the values of the received parameters and compares them with pre-defined threshold values. An optical link failure in the quantum channel or a disruption of the key-exchange service will result in higher QBER values and consequently lower SKR values or no key generation. Therefore, the QPM can decide to change the current QKD channel transmission path to a new secure operational path. This will be achieved with the assistance from the SDN controller, which will provide and configure an alternative optical path.

Regarding the SDN implementation, an extended

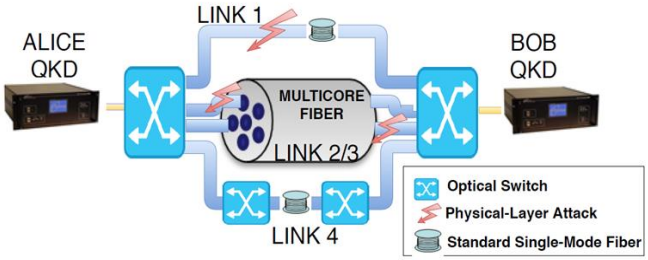

Fig. 4. Scenarios for the optical network

version of the OpenDaylight SDN controller is used with OpenFlow plugins that enable configuring the optical switches of the testbed. The SDN controller is also extended to communicate with the QPM application, which runs and monitors continuously the running QKD systems. The interface used for the communication between the SDN controller and the QPM is the REST API, as stated before. The SDN controller interfaces with a database (SQLite), which schema can be seen in Fig. 2. The database holds the information about all the alternative quantum channel paths between the different end-nodes of the QKD network. Specifically, the table fields are the names of the end-nodes of the path (sitename, connected_sitename), the distance between them (sitename) and all the connections between the optical switches in between them (optical_switch_left/ right_id and optical_switch_left/right_port), which need to be configured by the SDN controller.

Fig. 3 shows the flow and decision making of the QPM application. After a link failure, the QPM decides to change the quantum channel path, collecting a list of all the alternative paths for the quantum channel from the SDN controller. The QPM application chooses the alternative path from the database abovementioned. The information of the selected path is sent from the QPM application to the SDN controller for configuration through a REST API POST request. The SDN controller undertakes the respective configuration of the optical devices and sends an acknowledgment response to the QPM. Following the switching to the new path, the QKD devices will re-initialize and begin the key-exchange.

V. Scenarios for QKD Supported by SDN

From Fig. 1 it is clearly observed that the optical network enables the interconnection of the QKD units. This connectivity is critical for the key generation and distribution. In addition, any physical layer attack or "jamming" in the optical fiber links will be detrimental to the process of key distribution, where any interference with the encoded photons will be considered as an intruder in the connection and the key generation will be disrupted, compromising the security of the data transmission.

Fig. 4 shows the investigated link scenarios of an optical network with QKD resources. These scenarios are described as follows:

A. *Scenario 1*

The first scenario considers a link with a standard single-mode fiber (SSMF) interconnecting the QKD units via an optical fiber switch (Link 1, Fig. 4). This fiber switch represents the cross-connection in a reconfigurable optical add/drop multiplexer (ROADM) or an optical cross-connect (OXC) used in practical optical networks. Therefore, different paths can be used for network reconfigurability.

B. *Scenario 2*

The second scenario includes a 1km-long 7-core multicore fiber (MCF) with fan-in/fan-out interface. For this scenario, two links were considered, corresponding to two different cores of the MCF (Links 2 and 3 in Fig. 4).

C. *Scenario 3*

This last scenario includes additional optical fiber switches to represent a connection via multi-hop in the optical network (Link 4, Fig. 4). This kind of multi-hop configurations are typical of ring or mesh networks used in metropolitan or core networks.

VI. PHYSICAL-LAYER ATTACKERS

The scenarios of Fig. 4 show vulnerability to physical layer attacks and the "jamming" signal insertion attack is one of the most critical which may transform on a DoS of the users who rely on quantum encryption for the data communication. Two types of physical layer attacks are considered in here: *i)* an attack is directly aimed at the optical fiber link by inserting optical power via a 3-dB coupler (Fig. 5a) into the optical link and *ii)* an attack directly targets a MCF core corresponding to the quantum channel by injecting optical power in an adjacent core and inducing inter-core crosstalk (Fig. 5b). It is important to mention that the QKD system used [32] follows a two-way approach for passive autocompensation for fluctuations and that any attack over the QKD-Alice unit will be reflected back to the QKD-Bob unit, degrading the performance of the system and leading to keys not being generated. In addition, for the characterization of the attacked links, the inclusion of the optical switches was omitted, as shown in Fig. 5. Moreover, while DOS attacks can occur bi-directionally in QKD systems, in the present communication the attacks are undertaken in the direction to the QKD Alice unit. Detailed characterization of the attacks over the QKD Bob unit were undertaken in [22] and comparison of the simpler SMF case reveals negligible differences in the DOS behavior.

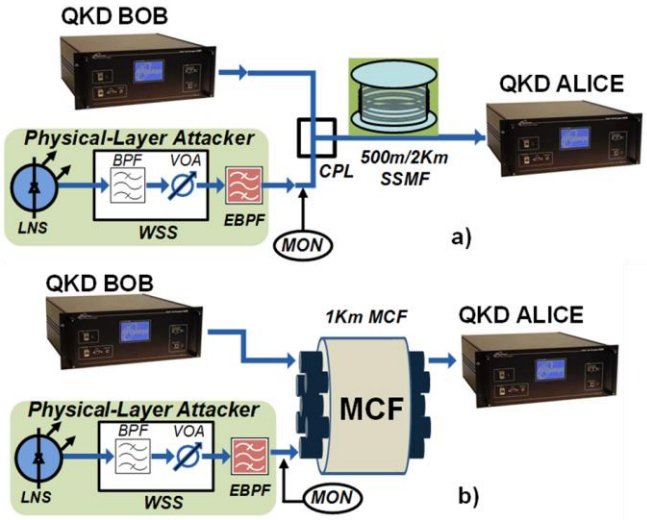

Fig. 5. Physical layer attackers for a) link 1 and b) link 2 and 3. **LNS**; Laser Noise Source, **WSS**: Wavelength Selective Switch, **BPF**: Band Pass Filter, **VOA**: Variable Optical Attenuator, **EBPF**: High-Edge Roll-Off BPF, **MCF**: Multicore Fiber, **CPL**: 3-dB Coupler, **MON**: Optical Power Monitor.

In both types of attackers, a tunable distributed feedback (DFB) laser source is used and its spectrum is limited by a bandpass filtering and attenuation function in a wavelength-selective switch (Finisar WaveShaper® 16000A). A band-pass filter with steeper roll-off edges was also used to further limit the Raman noise generated by the laser (Yenista XTM-50). This configuration allows an improved control of the amount of jamming optical power injected reflecting a less obvious attack, leading to a more active monitoring and programmability to mitigate the intrusion.

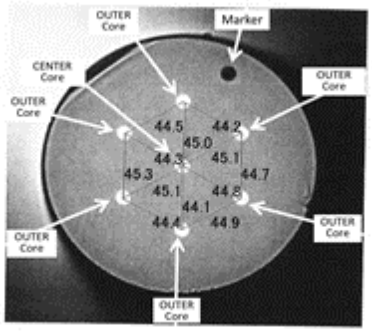

Fig. 6. Cross-sectional figure of the 7-core MCF used for the experimental system setup.

VII. EXPERIMENTAL RESULTS

A. *MCF CHARACTERISATION*

Fig. 6 shows the cross-sectional area of the MCF used. The MCF has an average core pitch of ~44.7 μm and a loss of 0.2 dB/km. Fig. 7 shows the measured static crosstalk between all the cores throughout the 1-km long MCF. Here a definition of the crosstalk is the ratio of the injected optical power on a selected core to the observed output power of another core. This resultant measured crosstalk

is the combination of the crosstalk observed in the MCF and the MCF fanouts. With this approximation, the location of a more suitable (i.e. less prone to crosstalk) core is possible for exchange of the QKD encoded photons.

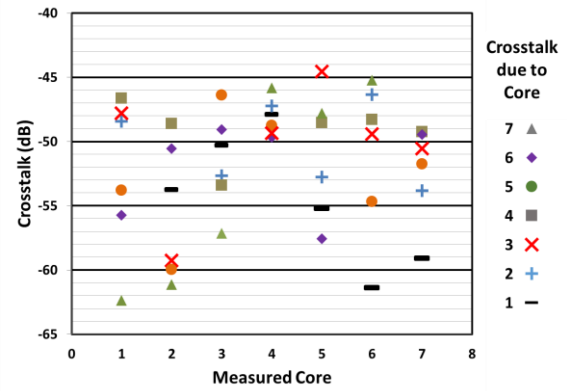

Fig. 7. Measured MCF Crosstalk @1552nm. (Measurement taken with OSA with dynamic range of >58 dB @0.4nm from peak wavelength and lowest optical sensitivity of -70 dBm)

The observed inter-core crosstalk for the MCF of Fig. 7 was statically characterized before the experiment was undertaken. However, as it is shown in [35], carrier-supporting signals may experience a strong dynamic time-dependence of inter-core crosstalk in a homogeneous multi-core fiber. Thus, the results plotted in Fig. 7 may have a fluctuation of >15 dB.

B. Physical layer intrusion evaluation of a SSMF link

To evaluate the impact of the physical layer attack over a SSMF link, Fig. 8 shows the SKR and QBER curves presented as a function of the optical power generated by the intruders into link 1 where the power is measured after the 3dB coupler (Fig. 5a). Two lengths of SSMF were selected: 500m and 2km. As it can be observed in Fig. 8, the SKR and QBER are kept within the limits of 1000b/s to 1250b/s and 2.2% to 3.2%, respectively, up to a measured power of -51dBm, for both cases of SSMF lengths.

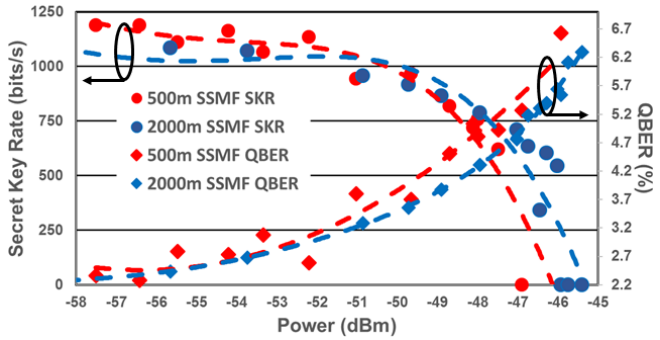

Fig. 8. Measured SKR and QBER vs injected optical power for the case of the physical layer attacker over link 1 (Fig. 4 and Fig. 5a). Measured power w/OSA Anritsu MS9710B, @0.07nm resolution, 70dB dynamic range). Dashed lines are polynomial fittings for the QBER and SKR curves

When the optical power added to link 1 through the 3dB coupler is higher than -51dBm, the SKR decreases and the QBER increases until the generation of keys is not possible, since the number of errors is beyond the correcting limit. For the case of the SSMF with 2km of length, the power reflected due to backscattering is ~1.5dBs higher than the case of the 500m of SSMF. This effect is reflected in the 1dB reduction of tolerance to injected power before the key generation is stopped (Fig. 8).

C. Physical layer intrusion evaluation of a MCF link

Fig. 9 illustrates the impact of inter-core crosstalk over a quantum channel. In here the core used for the transmission of the encoded photon is core 6 and the intrusion was added to core 7, denoting a crosstalk of ~45dB (Fig. 7). As observed, for an intruder input power higher than -28dBm, the inter-core crosstalk deteriorated the SKR and QBER up to a point where the generation of keys were impossible due to the high amount of errors induced by the optical power of the attacker in the adjacent core.

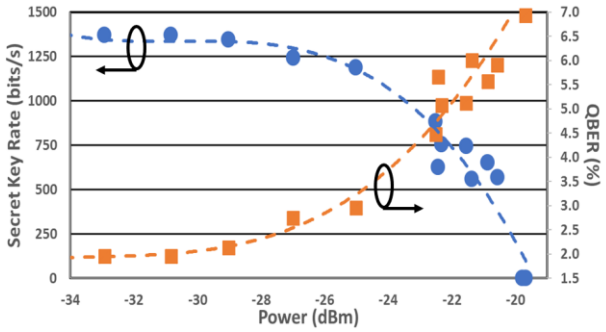

Fig. 9. Measured SKR and QBER vs optical power for the case of optical intrusion over an adjacent MCF core to the QKD channel core (link 2 Fig. 4 and Fig. 5b). Dashed lines are polynomial fittings for the QBER and SKR curves

To further understand the effect of crosstalk in the MCF, a common experimental setup shown in Fig. 10 was assembled. For the single core fiber study, the Quantum channel and the attacking CW wavelength are coupled through the 3dB coupler on the same core of the MCF, while for the case of MCF fiber study we launch the Quantum channel through the coupler (that is not bypassed) and the attacking CW is directly coupled on another core of the MCF. The injected optical power of the attacker for the case of single core is now measured in point B of the new experimental setup of Fig. 10 while the injected optical power for the case of MCF is taken in point A of Fig. 10. The total power loss in between the QKD Alice and Bob is 8dB for this testbed of Fig. 10. The measured SKR and QBER for the case of the SSMF and MCF are shown in Figs. 11 and 12, respectively. As observed in Figs. 11 and 12, the injection of power using an adjacent core allows more input power (up to -27dBm) compared to the case of the intruder with the 3dB coupler, where the injected power is -59dBm before the key generation is stopped. This difference of ~32dB is due to the inter-core crosstalk in the MCF in the selected cores.

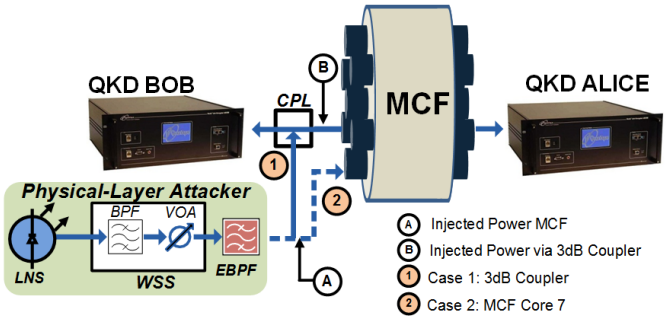

Fig. 10. Experimental setup for MCF crosstalk analysis with respect to scenario with 3dB coupler. Total new power loss in between Alice-Bob is 8dB.

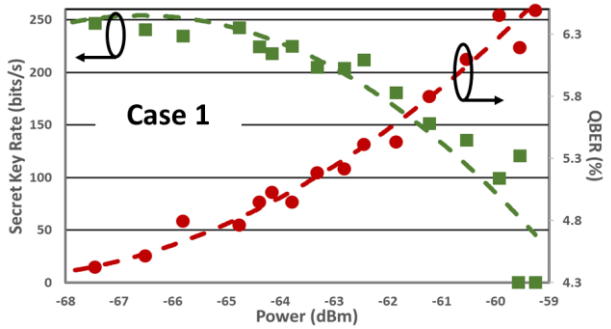

Fig. 11. SKR and QBER measured when intruder power is injected using a 3dB coupler (Fig. 10 testbed). Dashed lines are polynomial fittings for the QBER and SKR curves

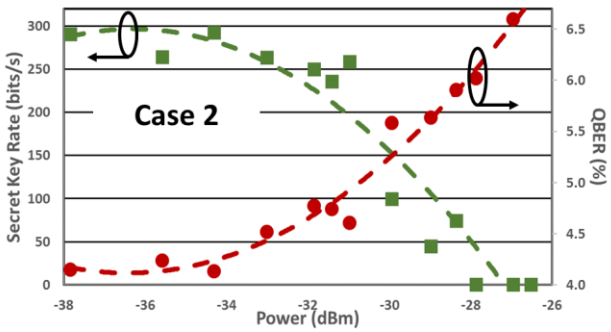

Fig. 12. SKR and QBER measured when intruder power is injected in adjacent core 7 (Fig. 10 testbed). Dashed lines are polynomial fittings for the QBER and SKR curves

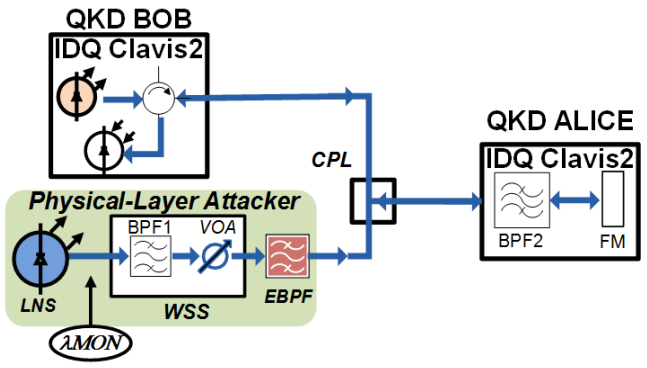

Fig. 13. Description of experimental testbed used to characterize the effect of the filter from the Physical-layer attacker. **BPF1:** Band-pass filter attacker (100GHz), **BPF2:** Band-pass filter QKD Alice unit (200GHz ITU). **EBPF:** High-Edge Roll-off BPF (150GHz). **FM:** Faraday Mirror

D. Wavelength tuning effect of the DOS attacker

In this section, the effect of tuning the wavelength of the laser source of the physical-layer attacker is investigated. Fig. 13 shows the testbed used and the location of the filters in the testbed. In this testbed, the total power loss between QKD Alice and Bob is 3dB. Fig. 14 illustrates the effect of tuning the wavelength of the attacker, considering an intrusive optical power QKD-Alice of -29.8dBm. For a center wavelength below 1551.8nm, the QKD system delivered a SKR and QBER of 2200b/s and 1.4%, respectively. When the wavelength is increased, secret keys are not generated in between the wavelengths of 1551.96nm and 1552.2nm (QBER were within the limits of 4.9% and 4.3%). For a wavelength higher than 1552.2nm, the QKD system generated keys and the performance of the system presented similar SKRs and QBERs compared to the ones obtained below the 1551.8nm wavelength. As observed in Fig. 14, the flat-top response of the QBER is a direct response of the combined EBPF and BPF2 filters of Fig. 13.

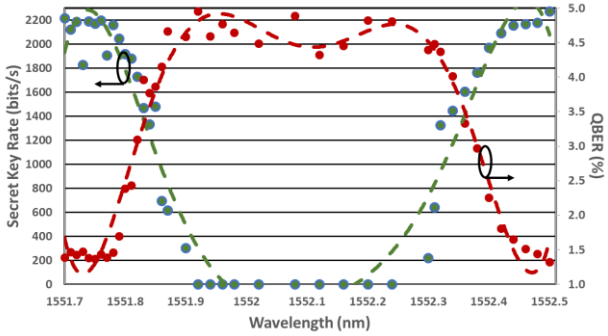

Fig. 14. Attacker wavelength tuning of the injected input power into the SSMF via a 3dB coupler. Dashed lines are polynomial fittings for the QBER and SKR curves

E. Performance evaluation of the QPM application and the SDN in mitigating the link failure

In this section, the latency measurements induced by the SDN architecture is presented to evaluate the effect of the QPM and SDN in the overall performance of the system. Specifically, the measured time for the process of link failure identification and re-allocation of the quantum channel path includes: *i)* the time required for the QPM application to identify the quantum link failure after the attack *ii)* the time for a REST API call to be sent from the QPM to the SDN controller, *iii)* the time needed for the SDN controller to send OpenFlow messages to the agent for optical switch configuration and, *iv)* the time undertaken by the optical switch to execute the suitable cross-connections required for link recovery (switching time of the optical switch ~10ms [36]).

Fig. 15 shows the measured times for different processes of the experiment. The times were measured for all the link failure cases (i.e. no key generation after the attack). Case 1 considers the failure happening in Link 1 and the SDN controller switches to Link 2. In Case 2 the failure happens in Link 2 and the controller switches to an adjacent low-inter-crosstalk core (core 1- Fig. 7) of the

MCF (Link 3). Lastly, Case 3 considers Link 2 being attacked and the path of Link 4 being selected for switching.

In Fig. 15 it is observed that the time required by the SDN controller to identify the link failure and setup the new optical path is negligible compared to the other processing times, i.e. the time required for the QKD units to re-initialize and generate a new key from the new path.

Process		Time (in sec)	Time (in min)
First initialization of the QKD units - First Key		480.46	8
Case 1: Link 1 to Link 2	Link Failure Identification / Re-allocation of Quantum Channel Path	0.056	0.00094
	Re-initialization of the QKD units - First Key from New Path	753.81	12.56
Case 2: Link 2 to Link 3	Link Failure Identification / Re-allocation of Quantum Channel Path	0.057	0.00095
	Re-initialization of the QKD Units - First Key from New Path	443.48	7.39
Case 3: Link 2 to Link 4	Link Failure Identification / Re-allocation of Quantum Channel Path	0.051	0.00085
	Re-initialization of the QKD Units - First Key from New Path	873.87	14.56

Fig. 15. Measured times for different processes of the QPM/ SDN architecture in case of a link failure.

The total time for the re-initialization after the change of optical path and until a new key is generated is longer than the first initialization times by additional ~4-6 minutes for the selected link processes, except for the Case 2. This derives from the fact that in Cases 1 and 3, the switching happens between two different links (i.e. two different SSMFs) with different losses and different optical fiber lengths (Table 1). This affects the initialization time for the QKD units since more time is required to synchronize and eventually generate keys from the new link. In the Case 2, Link 2 switches to Link 3, with the same length (~1km) and losses (~5.2dB) in both links (i.e. switching in between MCF cores), resulting in very close initialization times.

Though in our implementation the identification/re-allocation time from the SDN controller is 4 orders of magnitude lower than the re-initialization time required by the QKD equipment, the two timings can become comparable if the SKR is improved, as SKR also defines the execution times of the BB84 protocol. Four orders of magnitude improvement of the SKR compared to our current implementation of 1kb/s have already been demonstrated in [37], while additional improvements can be achieved by optimizing the re-initialization software stack.

Fig. 16 illustrates the time subdivision of the measured ~50ms for link failure identification/re-allocation of quantum channel path. As observed, 64% of the time is consumed during the REST API call sent from the QPM to the SDN controller. The remaining times are considered during SDN messaging to the optical switch, according to [38].

Process	Time (in msec)
Link Failure Identification	0.012
REST API call – QPM to SDN Controller	32
SDN message to Optical switch	6ms – 32ms [38]
Switching Time Optical switch	10

Fig. 16. Breakdown of times for identification-reallocation process in SDN controller.

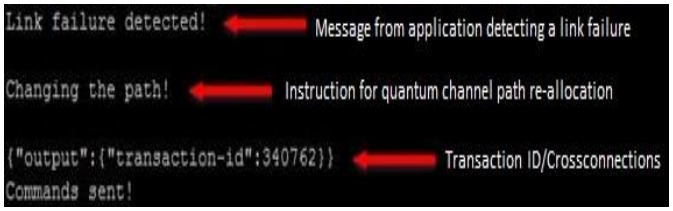

Fig. 17. Output of the QPM application in the moment a link failure is detected.

Fig. 17 shows the output of the QPM application software after a link failure is detected, triggered by the absence of key generation. Fig.17 depicts transaction IDs created corresponding to OpenFlow messages sent from the SDN controller to the optical switch, as shown in the Wireshark screenshot of Fig.18 for one transaction (ID 340762). Each transaction ID corresponds to a cross-connection in the optical switch resulting in a new quantum-secured path.

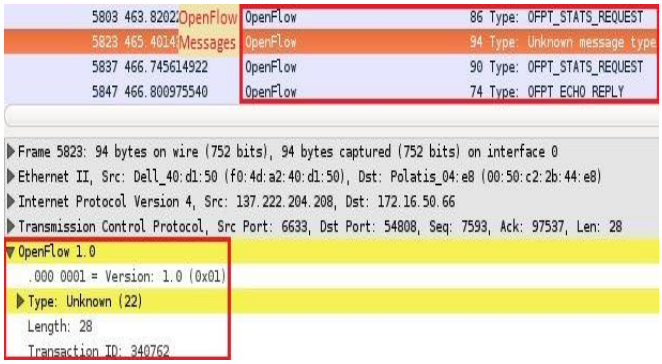

Fig. 18. Wireshark captured OpenFlow messages from one of the optical switches.

VIII. Conclusion

We experimentally demonstrate the mitigation of multiple link failure scenarios as a particular feature of an SDN-enabled QKD network. A monitoring SDN application was developed to monitor in real-time the quantum parameters of SKR and QBER and react in the event of lack of key generation or irregular QBER values, selecting an alternative route for the quantum channel. Four different quantum channel links (including SSMF and MCF) were applied in this experiment to investigate the different effects on the performance of the proposed integrated system. A study on the different types of

attackers and a characterization of the MCF links is presented, showing the level of sensitivity of the QKD system under different types of link failures. This investigation shows how a SDN framework with quantum-aware network control application, utilizing real-time monitoring of quantum parameters, can be successfully deployed in a QKD-enabled optical network. We demonstrated, using this framework, a secure data encryption scenario ensuring a continuous key generation service with insignificant delay regarding the link failure identification and re-allocation of secure quantum paths.

ACKNOWLEDGMENT

This work acknowledges EPSRC EP/M013472/1: UK Quantum Hub for Quantum Communications Technologies, EP/L020009/1: Towards Ultimate Convergence of All Networks and the EU Horizon 2020 METRO-HAUL project.

REFERENCES

[1] J. M. Simmons, Optical Network Design and Planning, 2nd ed., Springer, 2014.

[2] Cisco Global Cloud Index (2018). White Paper. [Online]. Available:https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/

[3] IDQuantique White Paper. "Fibre Optics Networks: Your Weakest Link". March 2011. [Online] Available: http://marketing.idquantique.com/acton/attachment/11868/f-0062/1/-/-/-/-/white-paper-optical-fibers.pdf

[4] UK Quantum Technology Hub for Quantum Communications Technologies. Annual Report 2016-2017.

[5] E. Diamanti, H.-K. Lo, B. Qi and Z. Yuan, "Practical challenges in quantum key distribution", *in Nature Photonics Journal Quantum Information.* Vol. 2, No. 16025; November 2016. pp. 1-12.

[6] R.Alléaume,et.al.,"Using quantum key distribution for cryptographic purposes: A survey", *in Theoretical Computer Science,* 560, (2014). pp. 62-81.

[7] P. Schartner and S. Rass, "Quantum key distribution and Denial-of-Service: Using strengthened classical cryptography as a fallback option", *in proceedings of International Computer Symposium (ICS)*, Taiwan, (2010). pp. 131-136.

[8] National Cyber Security Centre (GCHQ) White Paper. Quantum Key Distribution. October, 2016. [Online] Available: https://www.ncsc.gov.uk/whitepaper/quantum-key-distribution.

[9] M Peev, C. Pacher, R Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J-D Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J-B Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z L Yuan, H. Zbinden and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna", *in New J. Phys.* Vol. 11, No. 075001. 2009. pp. 1-37

[10] A. Wonfor et al., "High performance field trials of QKD over a metropolitan network", *in Proc. Qcrypt* (2017). Paper Th467.

[11] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network", *in Optics Express,* Vol. 22, No. 18, pp. 21739-21756.

[12] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network" *in Opt. Express,* vol. 19. no. 11. May. 2011. pp. 10387-10409.

[13] M. Channegowda, R. Nejabati, and D. Simeonidou, "Software-Defined Optical Networks Technology and Infrastructure: Enabling Software Defined Optical Network Operations [Invited]," *in J. Opt. Commun. Netw.,* vol. 5, no. 10, Oct. 2013. pp. A274-A282.

[14] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, N. M. Miller and Nao, "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks" *IEEE Communications Magazine*, Vol. 51, No. 7, Jul. 2013. pp. 36-43.

[15] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, A. Lord, R. Nejabati, and D. Simeonidou, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," *in J. Lightwave Technol.,* vol. 35, no. 8, Mar. 2017. pp. 1357–1362.

[16] A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez, and V. Martin, "Virtual Network Function Deployment and Service Automation to Provide End-to-End Quantum Encryption", *in J. Opt. Commun. Netw.* vol. 10, no. 4, pp. 421-430. Apr. 2018.

[17] A. Aguado, V. López, J. Martinez-Mateo, M. Peev, D. López and V. Martín, "VPN Service Provisioning via Virtual Router Deployment and Quantum Key Distribution", *in proceedings of Optical Fiber Communications conference (OFC),* San Diego, March, 2018. Th2A.32

[18] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez, and V. Martin, "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks", *in J. Opt. Commun. Netw.* vol. 9, no. 10, pp. 819-825. Oct. 2017.

[19] A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez and V. Martin, "GMPLS Network Control Plane Enabling Quantum Encryption in End-to-End Services", *in proceedings of International Conference on Optical Network Design and Modeling (ONDM),* Budapest, Hungary, May, 2017.

[20] A Aguado, J Martinez-Mateo, V Lopez, D Lopez, M Peev, V Martin, "Experimental Validation of an End-to-End QKD Encryption Service in MPLS environments", *7th International Conference on Quantum Cryptography (QCrypt 2017)*, Cambridge, UK. Sep. 2017. Th452.

[21] A. Aguado, V Martin, D Lopez, M Peev, J Martinez-Mateo, JL Rosales, F de la Iglesia, M Gomez, E Hugues-Salas, A Lord, R Nejabati, D Simeonidou "Quantum-Aware Software Defined Networks", *in proceedings of International Conference on Quantum Cryptography (QCrypt 2016),* Washington, D.C., USA. Sep. 2016.

[22] E. Hugues-Salas, F. Ntavou, Y. Ou, J. E. Kennard, C. White, D. Gkounis, K. Nikolovgenis, G. Kanellos, C. Erven, A. Lord, R. Nejabati and D. Simeonidou, "Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN)" *in proceedings of Optical Fiber Communications conference (OFC),* San Diego, March, 2018. M2A.6.

[23] K. A. Patel, J. F. Dynes, I. Choi, A.W. Sharpe, A. R. Dixon, Z. L. Yuan, R.V. Penty, and A. J. Shields, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber", *Physical Review X*, Vol. 2, No. 041010 (2012).

[24] J. F. Dynes, W. W-S. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards and A.

J. Shields, "Ultra-high bandwidth quantum secured data transmission", *Sci. Rep.* 6, 35149; (2016).

[25] D. J. Richardson, J. M. Fini, and L. E. Nelson, "Space-division multiplexing in optical fibres," *Nat. Photonics*. Vol 7, 2013. 354-362

[26] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R. V. Penty and A. J. Shields, "Quantum key distribution over multicore fiber", *in Optics Express*. Vol. 24, No. 8, April, 2016. pp. 8081-8087.

[27] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-Layer Security in Evolving Optical Networks", *IEEE Communications Magazine,* Vol. 54, No. 8, Aug. 2016. pp. 110-117.

[28] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, J. L. Marzo, "An overview of security challenges in communication networks", *in proceedings 8th International Workshop on Resilient Networks Design and Modeling (RNDM),* Halmstad, Sweden. Sep. 2016

[29] R. Goscien, C. Natalino, L. Wosinska and M. Furdek, "Impact of High-Power Jamming Attacks on SDM Networks", *in proceedings International Conference on Optical Network Design and Modeling (ONDM),* Dublin, Ireland, May 2018.

[30] J. Zhu and Z. Zhu, "Physical-Layer Security in MCF-Based SDM-EONs: Would Crosstalk-Aware Service Provisioning be Good Enough?", J. of Light. Tech, Vol. 35, No. 22, Nov. 2017. pp. 4826-4837.Yoshimichi Tanizawa, Ririka Takahashi, Hideaki Sato, Alexander R. Dixon, "An approach to integrate quantum key distribution technology into standard secure communication applications", *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 2017*

[31] A. Sano, H. Takara, T. Kobayashi, H. Kawakami, H. Kishikawa, T. Nakagawa, Y. Miyamoto, Y. Abe, H. Ono, K. Shikama, M. Nagatani, T. Mori, Y. Sasaki, I. Ishida, K. Takenaga, S. Matsuo, K. Saitoh, M. Koshiba, M. Yamada, H. Masuda and T. Morioka, "409-Tb/s + 409-Tb/s crosstalk suppressed bidirectional MCF transmission over 450 km using propagation-direction interleaving", *in Optics Express*, Vol. 21, No. 14. Jul. 2013. pp. 16777-16783.

[32] "ID Quantique Clavis2 QKD platform" [Online]. Available: https://www.idquantique.com/resource-library/quantum-key-distribution/

[33] "ID Quantique Centauris CN8000 platform" [Online]. Available: https://www.idquantique.com/resource-library/network-encryption/

[34] Y. Tanizawa, R. Takahashi, H. Sato, and A. R. Dixon, "An approach to integrate quantum key distribution technology into standard secure communication applications", *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 2017.*

[35] G. Rademacher, R. S. Luis, B. J. Puttnam, Y. Awaji and N. Wada, "Crosstalk dynamics in multi-core fibers", *in Optics Express,* Vol. 25, No. 10. May. 2017. pp. 12020-12028.

[36] S. Yan, E. Hugues-Salas, Y. Ou, R. Nejabati and D. Simeonidou, "Hardware-Programmable Optical Networks", *in Sci. China Inf. Sci.* No. 102301 Vol. 59. Sep. 2016. pp. 1–12.

[37] Z. L. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10 Mb/s quantum key distribution*", in J. Lightwave Technol.,* Vol. 36, No. 16. Aug. 2018. pp. 3427-3433.

[38] K. Hey, J. Khalidy, A. Gember-Jacobsony, S. Dasy, C. Prakashy, A. Akellay, L. E. Li and M. Thottan, "Measuring Control Plane Latency in SDN-enabled Switches", *in Proceedings of ACM SIGCOMM Symposium on SDN Research (SOSR)*, Santa Clara, CA, June 2015.